Journal of Algebra 357 (2012) 26–33

Contents lists available at SciVerse ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Irreducibility and embedding problems

Lior Bary-Soroker

Institut für Experimentelle Mathematik, Universität Duisburg–Essen, Ellernstrasse 29, D-45326 Essen, Germany

ARTICLE INFO

Article history:
Received 7 October 2010
Available online 2 March 2012
Communicated by Laurent Moret-Bailly

MSC:
12E30
12E25

Keywords:
Irreducible specializations
Pseudo algebraically closed extensions
Embedding problems

ABSTRACT

We study irreducible specializations, in particular when group-preserving specializations may not exist. We obtain a criterion in terms of embedding problems. We include several applications to analogs of Schinzel's hypothesis H and to the theory of Hilbertian fields.

1. Introduction

This paper deals with irreducible specializations: Given an irreducible and separable in X polynomial $f(T_1,\dots,T_r,X)\in K[\mathbf{T},X]$ over a field K we try to find a tuple $\mathbf{a}\in K^r$ such that $f(\mathbf{a},X)$ is irreducible in X. If every polynomial over K admits an irreducible specialization, then K is called Hilbertian.

In [1,4] several applications, to the theory of quadratic forms and to analogs of Dirichlet's theorem on primes in arithmetic progressions over polynomial rings, are obtained over fields that satisfy a weak irreducible specialization property. Namely, a certain subfamily of polynomials, the so-called "most-irreducible-polynomials", admits irreducible specializations. We say that M is a PAC (pseudo algebraically closed) extension of K, or in short that M/K is PAC, if $K\subseteq M$ and for every absolutely irreducible M-variety V of dimension $r\geqslant 1$ and for every dominating separable M-map $\nu: V\to\mathbb{A}^r$ there exists $\mathbf{a}\in V(M)$ such that $\nu(\mathbf{a})\in K^r$. A sufficient condition in terms of PAC extensions to have irreducible specializations for those "the-most-irreducible-polynomials" is obtained in [1]:

E-mail address: lior.bary-soroker@uni-due.de.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2012.01.024

Theorem 1.1. *Let K be a field and let $f(\mathbf{T}, X) \in K[\mathbf{T}, X]$ be a separable polynomial of degree n in X such that*

$$\mathrm{Gal}\big(f(\mathbf{T}, X), \tilde{K}(\mathbf{T})\big) \cong S_n.$$

Assume K has a PAC extension M having a separable extension N of degree $n = [N : M]$. Then there exists a Zariski dense set of $\mathbf{a} \in K^r$ such that $f(\mathbf{a}, X)$ is irreducible in $K[X]$.

Here $\tilde{K}$ denotes an algebraic closure of K.

In [4] Kelmer and the author prove that some interesting families of algebraic extensions of a countable Hilbertian field have PAC extensions with separable extension of degree $n \geqslant 5$, e.g. pro-solvable extensions, hence satisfy the conclusion of Theorem 1.1.

The goal of this paper is to vastly generalize Theorem 1.1 and to obtain new applications. To state the generalization we need to introduce the embedding problem associated to a polynomial: Let $f(\mathbf{T}, X) \in M[\mathbf{T}, X]$ be a polynomial over a field M that is separable in X. Let F be the splitting field of f over $M(\mathbf{T})$ and let N be the algebraic closure of M in F. Then $F/M(\mathbf{T})$ and N/M are Galois extensions and we have the canonical restriction maps

$$\begin{array}{ccc} & & \mathrm{Gal}(M) \\ & & \big\downarrow \rho \\ \mathrm{Gal}(F/M(\mathbf{T})) & \xrightarrow{\alpha} & \mathrm{Gal}(N/M). \end{array}$$

This diagram is an embedding problem for K which we call the *geometric embedding problem associated to f* and we denote it by $\mathcal{E}(f, M)$. A weak solution of the embedding problem is a homomorphism $\eta : \mathrm{Gal}(M) \to \mathrm{Gal}(F/M(\mathbf{T}))$ that commutes the diagram.

Proposition 1.2. *Let K be a field, $f_1(\mathbf{T}, X), \dots, f_s(\mathbf{T}, X) \in K[\mathbf{T}, X]$ non-associate irreducible polynomials that are separable in X, let $f = f_1 \cdots f_s$, and for each i let x_i be a root of $f_i(\mathbf{T}, X)$ in a fixed algebraic closure of $K(\mathbf{T})$. Assume there exist a PAC extension M/K, a subgroup $\ker\alpha \leqslant C \leqslant \mathrm{Gal}(f(\mathbf{T}, X), M(\mathbf{T}))$, and a weak solution $\eta : \mathrm{Gal}(M) \to \mathrm{Gal}(f(\mathbf{T}, X), M(\mathbf{T}))$ of $\mathcal{E}(f, M) = (\rho, \alpha)$ with image $H_0 = \eta(\mathrm{Gal}(M))$ such that*

$$(H_0 \cap C)x_i = Cx_i, \quad \text{for } i = 1, \dots, n.$$

Then there exists a Zariski dense set of $\mathbf{a} \in K^r$ such that all of the $f_i(\mathbf{a}, X)$ are irreducible over K.

Remark 1.3. Proposition 1.2 generalizes Theorem 1.1 since under Theorem 1.1, $\mathcal{E}(f, M) = (\mathrm{Gal}(M) \to 1, S_n \to 1)$. This embedding problem has a weak solution whose image is transitive if and only if M has a separable extension of degree n. Indeed, if $\alpha : \mathrm{Gal}(M) \to S_n$ is a homomorphism with a transitive image, then $\{\sigma \in \mathrm{Gal}(M) \mid \alpha(\sigma)(1) = 1\}$ is an open subgroup of $\mathrm{Gal}(M)$ of index n.

Remark 1.4. In the special case when K is a PAC field (i.e. $K = M$) and $C = \mathrm{Gal}(f(\mathbf{T}, X), M(\mathbf{T}))$, Proposition 1.2 becomes sharp, see [3, Theorem 2.4].

A first application is an analog of Schinzel's hypothesis H for polynomial rings:

Theorem 1.5. *Let K be a field of characteristic $p \geqslant 0$, let $n > 0$ be an integer such that n is odd if $p = 2$, and let $f_1(X), \dots, f_s(X) \in K[X]$ be non-associate irreducible separable polynomials with respective roots $\omega_1, \dots, \omega_s$. Assume there exists a PAC extension M/K such that $M(\omega_i)$ has a degree n separable extension, for every $i = 1, \dots, s$. Then there exists a Zariski dense set of $(a_1, \dots, a_n) \in K^n$ such that for $g(T) = T^n + a_1 T^{n-1} + \cdots + a_n$ all of the $f_i(g(T))$ are irreducible over K.*

We note that over finite fields a similar theorem was proved with an asymptotic formula, see [7] and [3]. Over PAC fields (i.e., when $M = K$) the theorem is sharp, see [3].

The second result concerns Hilbertian fields:

Theorem 1.6. *Let K be a field. Assume that for infinitely many $n \geqslant 1$ there exists a PAC extension M/K with $\mathrm{Gal}(M)$ free of rank $\geqslant n$. Then K is Hilbertian.*

This generalizes a result of Razon asserting that if K has a PAC extension with $\mathrm{Gal}(M)$ free of infinite rank, then K is Hilbertian [8, Corollary 2.6].

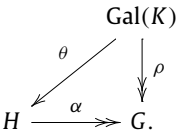
Note that if K is Hilbertian and countable, then for every integer n, there exists a PAC extension M/K with $\mathrm{Gal}(M)$ free of rank n [6].

2. Preparations

We briefly recall the definitions of geometric embedding problems and of double embedding problems and formulate the lifting property of PAC extensions. This property plays a crucial role in the proof of Proposition 1.2. Full details appear in [2], cf. [3].

2.1. Geometric embedding problems

Let K be a field, K_s a separable closure of K, and $\mathrm{Gal}(K) = \mathrm{Gal}(K_s/K)$ the absolute Galois group of K. A finite embedding problem $\mathcal{E}$ for K consists on an epimorphism of finite groups $\alpha : H \to G$ and an epimorphism[1] $\rho : \mathrm{Gal}(K) \to G$. In short we write $\mathcal{E} = (\rho, \alpha)$. A weak solution is a homomorphism $\theta : \mathrm{Gal}(K) \to H$ such that $\alpha \circ \theta = \rho$. If θ is surjective, we say that θ is a proper solution.



Assume that E is a finitely generated regular extension of K, and let F/E be a finite Galois extension. Then $L = F \cap K_s$ is Galois over K and

$$\mathcal{E}(F/E, K) = \big(\rho : \mathrm{Gal}(K) \to \mathrm{Gal}(L/K), \alpha : \mathrm{Gal}(F/E) \to \mathrm{Gal}(L/K)\big),$$

with ρ, α the restriction maps, is a finite embedding problem for K (note that E/K regular implies that α is surjective). We say that $\mathcal{E}(F/E, K)$ is a *geometric* embedding problem for K. If $E = K(\mathbf{T})$ for some tuple $\mathbf{T} = (T_1, \ldots, T_r)$ of algebraically independent variables, we call the embedding problem $\mathcal{E}(F/K(\mathbf{T}), K)$ *rational*.

Let φ be a K-place of E (thus, $\varphi(x) = x$, for all $x \in K$). Assume that the residue field of φ is K and that φ is unramified in F. Then for every L-place Φ of F that extends φ there exists a unique weak solution Φ^* of $\mathcal{E}(F/E, K)$ that satisfies

$$\Phi\big(\Phi^*(\sigma)x\big) = \sigma\,\Phi(x), \tag{1}$$

for every $\sigma \in \mathrm{Gal}(K)$ and for every $x \in F$ with $\Phi(x) \neq \infty$. (Indeed, consider the canonical exact sequence $1 \to I_\Phi \to D_\Phi \to G_\Phi \to 1$, where I_Φ is the inertia group, D_Φ the decomposition group and $G_\Phi = \mathrm{Gal}(\bar{F}/K)$ the Galois group of the residue field extension $\bar{F}/K$. Then the assumption that φ is unramified in F implies that $I_\Phi = 1$, hence $\nu : D_\Phi \to G_\Phi$ is injective. Thus (1) gives that Φ^* must be the composition of the restriction map $\mathrm{Gal}(K) \to G_\Phi$ and $\nu^{-1} : G_\Phi \to D_\Phi$.)

[1] All homomorphisms are assumed to be continuous.

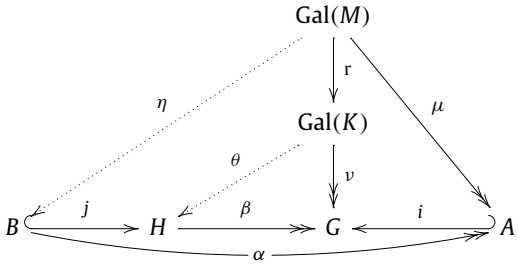
If $\tau \in \ker(\alpha) = \mathrm{Gal}(F/EL)$, then $\Phi \circ \tau$ is also an L-place of F that extends φ. The associated weak solution of $\mathcal{E}(F/E, K)$ is $(\Phi^*)^\tau$ defined by $(\Phi^*)^\tau(\sigma) = \tau^{-1}\Phi^*(\sigma)\tau$. Thus, the collection $\varphi^* = \{\Phi^* \mid \Phi \text{ is an } L\text{-place that extends } \varphi\}$ is a $\ker\alpha$-automorphism class.

When $E = K(\mathbf{T})$, $\mathbf{T} = (T_1, \dots, T_r)$, $r \geqslant 1$, and F is the splitting field over E of a polynomial $f(\mathbf{T}, X)$ that is separable in X, we write $\mathcal{E}(f, K) = \mathcal{E}(F/E, K)$ and say that $\mathcal{E}(f, K)$ is the *associated embedding problem*. We emphasize that in this case $\mathrm{Gal}(F/E) = \mathrm{Gal}(f, K(\mathbf{T}))$ comes together with a natural action on the roots of f, hence with a permutation representation of degree $\deg_X f$.

Remark 2.1. Let $\mathbf{a} \in K^r$ be such that $f(\mathbf{a}, X)$ is separable and of the same degree as the X-degree of $f(\mathbf{T}, X)$. Extend $\mathbf{T} \mapsto \mathbf{a}$ to a K-place of $K(\mathbf{T})$ with residue field K [5, Example 2.6.10] and let Φ be an L-place of F extending φ. Then $\Phi(x) \neq \infty$, for every root $x \in F$ of $f(\mathbf{T}, X)$. By (1) the map $\Phi^* : \mathrm{Gal}(K) \to \mathrm{Gal}(f(\mathbf{T}, X), K(\mathbf{T}))$ respects the actions of $\mathrm{Gal}(K)$ on the roots of $f(\mathbf{a}, X)$ and of $\mathrm{Gal}(f(\mathbf{T}, X), K(\mathbf{T}))$ on the roots of $f(\mathbf{T}, X)$.

2.2. Double embedding problems

Let M/K be a field extension. A *finite double embedding problem* consists of a commutative diagram

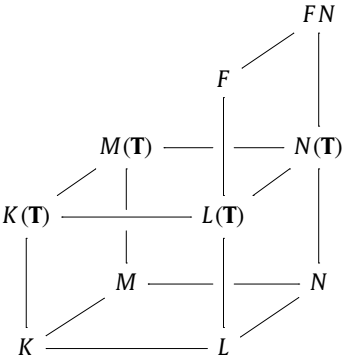


(2)

where G, H, A, B are finite groups, $B \leqslant H$, $A \leqslant G$, i, j are the inclusion maps, r is the restriction map, and α, μ, β, ν are surjective. (Note that if M/K is not algebraic, then r is not necessarily injective.) Therefore a finite double embedding problem consists of two compatible finite embedding problems: (ν, β) for K and (μ, α) for M. In short, we denote the double embedding problem by $((\mu, \alpha), (\nu, \beta))$.

A weak solution is a pair (η, θ) consisting of a weak solution η of (μ, α) and a weak solution θ of (ν, β) that commute (2). We note that $\eta = \theta \circ \mathrm{r}$, and that $(\theta \circ \mathrm{r}, \theta)$ is a weak solution if and only if $\theta(\mathrm{r}(\mathrm{Gal}(M))) \leqslant B$.

A finite double embedding problem is called *rational* if (ν, β) is rational. In that case, $H = \mathrm{Gal}(F/K(\mathbf{T}))$ for some Galois extension $F/K(\mathbf{T})$, $G = \mathrm{Gal}(L/K)$, where $L = F \cap K_s$, and β, ν are the restriction maps.



Then $G = \mathrm{Gal}(L/K)$, $H = \mathrm{Gal}(F/K(\mathbf{T}))$, $A = \mathrm{Gal}(L/L\cap M) \cong \mathrm{Gal}(N/M)$, where $N = LM$, and B is a subgroup of $\beta^{-1}(A) = \mathrm{Gal}(FN/M(\mathbf{T}))$. So $B \cong \mathrm{Gal}(FN/E)$, for some $M(\mathbf{T}) \subseteq E \subseteq FN$. Under this identifications, α becomes the restriction map. Note that since α is surjective, $E \cap M_s = M$, and thus E is regular over M. So (μ, α) is a geometric embedding problem.

A *geometric weak solution* of a rational double embedding problem consists of a pair (Ψ^*, Φ^*), where Ψ is an N-place of FN unramified over $M(\mathbf{T})$ such that the residue field of $K(\mathbf{T})$ is K, $\Phi = \Psi|_F$, and the residue fields of FN is the compositum of N with the residue field of F. In particular, Φ^* is a geometric weak solution of (ν, β).

We note that if $f(\mathbf{T}, X) \in K[\mathbf{T}, X]$ is a separable polynomial, then $\mathcal{E}(f, M/K) = (\mathcal{E}(f, M), \mathcal{E}(f, K))$ is a finite rational double embedding problem for M/K.

2.3. The lifting property

We formulate the lifting property of PAC extensions [2, Proposition 4.6].

Proposition 2.2. *Let M/K be a PAC extension, let*

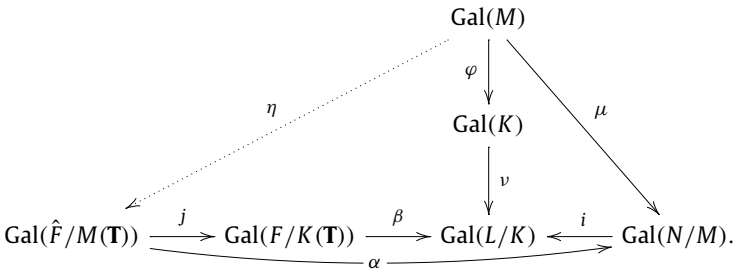
$$(\mathcal{E}_M, \mathcal{E}_K) = \big(\big(\mu : \mathrm{Gal}(M) \to A, \alpha : B \to A\big), \big(\nu : \mathrm{Gal}(K) \to G, \beta : H \to G\big)\big)$$

be a rational finite double embedding problem for M/K and let η be a weak solution of $\mathcal{E}_M$. Then there exists a geometric weak solution (Ψ^*, Φ^*) of $(\mathcal{E}_M, \mathcal{E}_K)$ such that $\Psi^* = \eta$.

Moreover, if $H = \mathrm{Gal}(F/K(\mathbf{T}))$, $\mathbf{T} = (T_1, \dots, T_r)$, and if $q(\mathbf{T}) \in K[\mathbf{T}]$ is nonzero, then we can choose Ψ so that $\mathbf{a} = \Psi(\mathbf{T}) \in K^r$, and $q(\mathbf{a}) \neq 0$.

3. Proof of Proposition 1.2

Let K be a field, $\mathbf{T} = (T_1, \dots, T_r)$, and $0 \neq q(\mathbf{T}) \in K[\mathbf{T}]$. Let $f_1(\mathbf{T}, X), \dots, f_s(\mathbf{T}, X) \in K[\mathbf{T}, X]$ be non-associate irreducible polynomials that are separable in X, $f = f_1 \cdots f_s$, and for each i let x_i be a root of $f_i(\mathbf{T}, X)$ in a fixed algebraic closure of $K(\mathbf{T})$. Let F be the splitting field of $f(\mathbf{T}, X)$ over $K(\mathbf{T})$, then $\hat{F} = FM$ is the splitting field of $f(\mathbf{T}, X)$ over $M(\mathbf{T})$. Let $L = F \cap K_s$ and $N = LM = FM \cap K_s$. Then the associated double embedding problem $\mathcal{E}(f, M/K) = (\mathcal{E}(f, M), \mathcal{E}(f, K))$ is



Here all of the maps are restriction maps. Note that $\hat{F} = FN$ and $\ker(\alpha) \cong \ker(\beta) \cong \mathrm{Gal}(FK_s/K_s(\mathbf{T}))$.

Assume we are given a weak solution $\eta : \mathrm{Gal}(M) \to \mathrm{Gal}(\hat{F}/M(\mathbf{T}))$ of $\mathcal{E}(f, M)$. Let $H_0 = \eta(\mathrm{Gal}(M))$ be the image of η. By the lifting property there is an $\mathbf{a} \in K^r$ and a geometric weak solution (Ψ^*, Φ^*) of $\mathcal{E}(f, M/K)$ such that $\Phi(\mathbf{T}) = \Psi(\mathbf{T}) = \mathbf{a}$, $q(\mathbf{a}) \neq 0$, $f(\mathbf{a}, X)$ is separable, $\deg(f(\mathbf{a}, X)) = \deg_X f(\mathbf{T}, X)$, and $\Psi^* = \eta$. Let $H_1 = \Phi^*(\mathrm{Gal}(K))$; then $H_0 \leqslant H_1 \leqslant H := \mathrm{Gal}(F/K(\mathbf{T}))$. It follows that each $f_i(\mathbf{a}, X)$ is separable and $\deg(f_i(\mathbf{a}, X)) = \deg_X(f_i(\mathbf{T}, X))$.

For each i, the polynomial $f_i(\mathbf{a}, X)$ is irreducible over K if and only if $\mathrm{Gal}(K)$ acts transitively on the set of roots of $f_i(\mathbf{a}, X)$ for all i. By Remark 2.1 the action of $\mathrm{Gal}(K)$ on the roots of $f(\mathbf{a}, X)$ is transposed to the action of H_1 on the roots of $f(\mathbf{T}, X)$. So it suffices to prove that, for each i, H_1 acts transitively on the set of roots of $f_i(\mathbf{T}, X)$, namely on Hx_i.

By assumption there exists $\ker\alpha \leqslant C \leqslant \mathrm{Gal}(f(\mathbf{T}, X), M(\mathbf{T}))$ and a weak solution η such that

$$(H_0 \cap C)x_i = Cx_i, \quad i = 1, \dots, s. \tag{3}$$

Let $hx_i \in Hx_i$. Since $\beta(H_1) = \nu(\mathrm{Gal}(K)) = \mathrm{Gal}(L/K)$, we have $h_1 \in H_1$ such that $h_1^{-1}h \in \ker\beta = \ker\alpha \leqslant C$. By (3), there exists $c \in H_0 \cap C$ such that $h_1^{-1}hx_i = cx_i$, hence $hx_i = (h_1c)x_i$. This finishes the proof since $h_1c \in H_1(H_0 \cap C) \leqslant H_1$. □

4. Applications

Recall the definition of the permutational wreath product: Let G, H be finite groups that act on finite sets X, Y, respectively. Then H acts on G^Y, and we define the permutational wreath product $G \wr_Y H$ to be the semidirect product $G^Y \rtimes H$. It comes with an action on $X \times Y$: if $f \in G^Y$, $h \in H$, $x \in X$ and $y \in Y$, then $(f, h)(x, y) = (f(hy)x, hy)$. If G, H are permutation groups (i.e. both actions are faithful), then one can show that $G \wr_Y H$ is a permutation group on $X \times Y$.

4.1. Proof of Theorem 1.5

Let K be a field of characteristic $p \geqslant 0$, let $n \geqslant 1$ be an integer such that n is odd if $p = 2$, and let $f_1(X), \dots, f_s(X) \in K[X]$ be non-associate irreducible separable polynomials with respective roots $\omega_1, \dots, \omega_s$. Assume there exists a PAC extension M/K such that $M(\omega_i)$ has a degree n separable extension, $i = 1, \dots, s$. We wish to prove that there exists a Zariski dense set of $(a_1, \dots, a_n) \in K^n$ such that for $g(T) = T^n + a_1T^{n-1} + \cdots + a_n$ each of the $f_i(g(T))$ is irreducible over K.

Let $f = f_1 \cdots f_s$, let $\mathbf{A} = (A_1, \dots, A_n)$ be an n-tuple of algebraically independent variables and let

$$\mathcal{G}(\mathbf{A}, T) = T^n + A_1T^{n-1} + \cdots + A_n.$$

Let F be the splitting field of $f \circ \mathcal{G}(\mathbf{A}, T)$ over $K(\mathbf{A})$ and L be the splitting field of f over K. Then since n is odd if $p = 2$, [3, Proposition 3.6] gives that F is regular over L and

$$\mathrm{Gal}\big(F/K(\mathbf{A})\big) \cong S_n \wr_\Omega \mathrm{Gal}(L/K),$$

as permutation groups. Here the left-hand side acts on the set Φ of roots of $f \circ \mathcal{G}(\mathbf{A}, T)$ in some algebraic closure of $K(\mathbf{A})$, $S_n \wr_\Omega \mathrm{Gal}(L/K)$ is the permutational wreath product that acts on the set $\{1, \dots, n\} \times \Omega$, where Ω is the set of roots of f, as defined in the first paragraph of Section 4.

Similarly $\mathrm{Gal}(f \circ \mathcal{G}(\mathbf{A}, T), M(\mathbf{A})) = \mathrm{Gal}(FM/M(\mathbf{A})) = S_n \wr_\Omega \mathrm{Gal}(N/M)$, where $N = LM$ is the splitting field of f over M. So

$$\mathcal{E}(f \circ \mathcal{G}, M) = \big(\nu : \mathrm{Gal}(M) \to \mathrm{Gal}(N/M), \alpha : S_n \wr_\Omega \mathrm{Gal}(N/M) \to \mathrm{Gal}(N/M)\big),$$

where α is the quotient map. Note that $\ker\alpha = S_n^\Omega$.

Let $\Omega_1, \dots, \Omega_{s'}$ be the $\mathrm{Gal}(N/M)$-orbits of Ω, so $s' \geqslant s$. Without loss of generality assume that $\omega_i \in \Omega_i$, for $i = 1, \dots, s$. By assumption, for each $i = 1, \dots, s$, we have a tower of separable extensions $M \subseteq M(\omega_i) \subseteq M_i$ and $[M_i : M(\omega_i)] = n$. For $i = s + 1, \dots, s'$, let $M_i = M(\omega_i)$, for some $\omega_i \in \Omega_i$.

Let $\hat{M}$ be the minimal Galois extension of M that contains all M_i. In particular $\hat{M}$ contains N. Then by [3, Lemma 3.7] we have a homomorphism $\rho : \mathrm{Gal}(\hat{M}/M) \to S_n \wr_\Omega \mathrm{Gal}(N/M)$ such that:

(a) $\alpha(\rho(\sigma)) = \sigma|_N$.
(b) Denote by H_0 the image of ρ. Then H_0 acts transitively on $\{1, \dots, n\} \times \Omega_i$, for $i = 1, \dots, s$.

Let C be the subgroup of all elements of $S_n \wr_\Omega \mathrm{Gal}(N/M)$ that leave each of the sets $\{1,\dots,n\}\times\Omega_i$ invariant, $i=1,\dots,s$. Then $\ker\alpha = S_n^\Omega \leqslant C$ and $H_0 \leqslant C$. In particular, $H_0 \cap C = H_0$, which explains the first equality in (4).

$$(H_0\cap C)(1,\omega_i) = H_0(1,\omega_i) = \{1,\dots,n\}\times\Omega_i = C(1,\omega_i), \quad i=1,\dots,s. \tag{4}$$

The second equality follows from the transitivity property (b) above, and the third one follows from the transitivity of H_0 combined with the definition of C. By Proposition 1.2, there exists a Zariski dense set of $\mathbf{a}\in K^n$ such that all $f_i(g(T))$ are irreducible, where $g(T)=\mathcal{G}(\mathbf{a},T)=T^n+a_1T^{n-1}+\cdots+a_n$. □

4.2. Proof of Theorem 1.6

Let K be a field. Assume that for infinitely many $n\geqslant 1$ there exists a PAC extension M/K with $\mathrm{Gal}(M)$ free of rank $\geqslant n$. We have to show that K is Hilbertian.

Let $f(T,X)\in K[T,X]$ be an irreducible polynomial that is separable and of degree $n\geqslant 1$ in X. By assumption, there exists a PAC extension M/K such that $\mathrm{Gal}(M)$ is a free profinite group of rank $r\geqslant n!$. In particular $r\geqslant \mathrm{rank}(\mathrm{Gal}(f(T,X),M(T)))$, so the associated embedding problem

$$\mathcal{E}(f,M)=\big(\nu:\mathrm{Gal}(M)\to\mathrm{Gal}(N/M),\alpha:\mathrm{Gal}\big(f(T,X),M(T)\big)\to\mathrm{Gal}(N/M)\big)$$

is properly solvable [5, Proposition 17.7.3 and Theorem 24.8.1], so by Proposition 1.2 (see Remark 1.3) there exists an element $a\in K$ for which $f(a,X)$ is irreducible. Thus K is Hilbertian. □

5. On the condition of Proposition 1.2

To get the conclusion of Proposition 1.2 we need to find a PAC extension M/K, a subgroup C with certain properties. Here are two special cases when there exists such a subgroup.

Case 1: Transitive solution Assume that the associated embedding problem $\mathcal{E}(f,M)$ has a weak solution η with image H_0 such that for each i, H_0 acts transitively on the roots of $f_i(\mathbf{T},X)$. Then if we take $C=\mathrm{Gal}(f,M(\mathbf{T}))$, we get that $(H_0\cap C)x_i = H_0x_i$ is the set of all roots of $f_i(\mathbf{T},X)$ and thus also Cx_i. In particular those are equal.

Note that in such a case $f_i(\mathbf{T},X)$ is irreducible over $M(\mathbf{T})$, $i=1,\dots,n$.

Case 2: Proper solution Assume that the associated embedding problem $\mathcal{E}(f,M)$ has a proper solution η. Denote the image of η by H_0. Then if we take $C=\ker\alpha$, then $C\subseteq H_0=C$, and hence $C\subseteq H_0x_i = Cx_i$.

Note that in this case $f_i(\mathbf{T},X)$ do not have to be irreducible over M.

Acknowledgments

The author wish to thank Moshe Jarden for many helpful remarks that improved the presentation of this paper.

The author was partially supported by the Lion foundation.

References

[1] Lior Bary-Soroker, Dirichlet's theorem for polynomial rings, Proc. Amer. Math. Soc. 137 (1) (2009) 73–83.
[2] Lior Bary-Soroker, On pseudo algebraically closed extensions of fields, J. Algebra 322 (6) (2009) 2082–2105.
[3] Lior Bary-Soroker, Irreducible values of polynomials, Adv. Math. 229 (2) (2012) 854–874.
[4] Lior Bary-Soroker, Dubi Kelmer, On PAC extensions and scaled trace forms, Israel J. Math. 175 (1) (2010) 113–124.
[5] Michael D. Fried, Moshe Jarden, Field Arithmetic, third ed., Ergeb. Math. Grenzgeb. (3) (Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics), vol. 11, Springer-Verlag, Berlin, 2008, revised by Jarden, MR MR2445111.

[6] Moshe Jarden, Aharon Razon, Pseudo algebraically closed fields over rings, Israel J. Math. 86 (1–3) (1994) 25–59, MR MR1276130 (95c:12006).
[7] Paul Pollack, Simultaneous prime specializations of polynomials over finite fields, Proc. Lond. Math. Soc. (3) 97 (3) (2008) 545–567, MR MR2448239 (2009f:11155).
[8] Aharon Razon, Abundance of Hilbertian domains, Manuscripta Math. 94 (4) (1997) 531–542, MR MR1484642 (98h:12002).